Comments of the California Office of Privacy Protection on the *Model Policy on Public Access to Court Records*

Draft dated February 22, 2002
Prepared on behalf of the Conference of Chief Justices
and the Conference of State Court Administrators
by the National Center for State Courts and the Justice Management Institute

---

Introduction

The California Office of Privacy Protection, in the California Department of Consumer Affairs, is a state office with the statutory mission of protecting the privacy rights of Californians. First funded in July 2001, the Office provides assistance to victims of identity theft and other consumers with privacy concerns, conducts public education and information programs on privacy issues, coordinates with law enforcement on investigations of identity theft and other privacy-related crimes, and makes recommendations to organizations for policies and practices that promote and protect the privacy interests of California consumers. It is in this latter capacity that the Office submits the following comments on the *Model Policy on Public Access to Court Records.*

The balancing of the competing values of public access to government records with individual privacy rights is one of the most significant public policy issues Americans face today. While the issue is not a new one, its importance and complexity have been increased in recent years by the proliferation of electronic databases of personal information on individuals. Government and the courts have moved to digital records and adopted "e-government" strategies to streamline operations and facilitate public access, putting more and more records on web sites. A new industry has sprung up to exploit electronic public records. Some information brokers buy public records from government agencies, sometimes purchasing entire databases (for example, all the birth and death records of Californians, or all the property records of a given county). Some government agencies even provide comprehensive databases of public records in convenient CD-ROM format, for a fee. Information brokers may "enrich" the data they purchase by combining several different databases, and then they may resell them to marketers, private investigators and others, and even back to government agencies.

Public records contain a wealth of personal information, information that in most cases was collected under compulsion. This information clearly has great value—to information brokers and marketers, and also to identity thieves. The uncontrolled distribution and redistribution of personal information, much of it from public records, has undoubtedly contributed to the epidemic status of identity theft, which is often cited as the fastest-growing crime in the nation. One recent study estimates that one in 50 Americans was a victim of identity theft in the past year, while one in 12 have been victims in their lifetime.[1]

[1] "Identity Theft: The Most Personal Privacy Violation," Gartner, Inc., March 8, 2002.

Court records are particularly sensitive, because they may contain some of the most deeply personal and intimate information about individuals. Any policies that would have the impact of increasing the exposure of these records to public view and commercial use are deserving of thoughtful and deliberate consideration. We commend the Conference of Chief Justices and the Conference of State Court Administrators for appointing an advisory committee to consider the issues involved in developing the Model Rule, and particularly for including at least one privacy rights advocate on the committee.

The Office respectfully submits the following comments, in which we express concern over the privacy implications of some of the rules in the model policy. As more fully set forth below, the Office is primarily concerned that proposed Rule 4.40, the model bulk distribution rule, threatens to impair the privacy rights of litigants and other voluntary and involuntary participants in the judicial system; provides little benefit to that system; and, at the same time, threatens to impose significant burdens on the system. The Office also believes that proposed Rule 8.10, on notice to litigants, fails to provide essential information regarding litigants' rights to seek limitations on the access to, and distribution of, their personal information.

Regarding Proposed Rule 4.40 – Requests for Bulk Distribution of Court Records in Electronic Form

Proposed Rule 4.40 would allow distribution of court records in bulk form. The Office believes that only electronic court calendars, registers of actions, and indices should be distributed in bulk. The Office believes that any other court records determined to be appropriate for electronic distribution should be available only on a case-by-case basis pursuant to specific identification and request, and, in addition, that electronic records in "sensitive" cases should be available only at the courthouse. These principles are derived from California Rules of Court 2070-2076, which are described more fully below.

The Office recognizes that, in time, reliable automated methods of redacting personal information from court records may become widely available and commonly used. At that time, the Office would support reevaluating the limitations on bulk distribution of electronic court records that are described in these comments.

CALIFORNIA RULES OF COURT

We recommend the approach taken by the California Judicial Council, which recently adopted rules on Public Access to Electronic Trial Court Records (California Rules of Court, Rules 2070 through 2076, effective July 1, 2002). In the words of the Court Technology Advisory Committee, which recommended the new rules to the Judicial Council, "the rules establish

statewide policies on public access to trial courts' electronic records that provide reasonable electronic access while protecting privacy and other legitimate interests."[2]

The California Rules apply to trial court records maintained in electronic form, but do not require courts to maintain records in electronic form. Under the Rules, a court that maintains registers of actions, calendars and indices electronically must provide electronic access to them, both remotely and at the courthouse. (Rule 2073(b)(1).) These records also may be distributed in bulk. (Rule 2073(f).) Courts that maintain electronic records in the following kinds of sensitive cases must provide electronic access to them, but only at the courthouse. These cases are:

- Proceedings under the Family Code;
- Juvenile court proceedings;
- Guardianship or conservatorship proceedings;
- Mental health proceeding;
- Criminal proceeding; and
- Civil harassment proceeding. (Rule 2073(c).)

Courts that maintain electronic records in other kinds of civil cases must provide electronic access to them both remotely and at the courthouse. (Rule 2073(b)(2).) However, a court may grant electronic access to an electronic record in any kind of case only when the case is specifically identified, and only on a case-by-case basis. (Rule 2073(e).) Bulk distribution of electronic case records in any kind of case is not permitted. (Rules 2073(e),(f).)

The Court Technical Advisory Committee explained Rule 2073 as follows:

> "The rule allows a level of access to all electronic records that is at least equivalent to the access that is available for paper records and, for some types of records, is much greater. At the same time, it seeks to protect legitimate privacy concerns.
>
> Family law, juvenile, guardianship/conservatorship, mental health, criminal, and civil harassment proceedings are excluded] from remote electronic access. The committee recognized that while these case records are public records and should remain available at the courthouse, either in paper or electronic form, they often contain sensitive personal information. The court should not publish that information over the Internet.
>
> [Other subdivisions of Rule 2073] limit electronic access to records (other than the register, calendars, or indexes) to a case-by-case basis and prohibit bulk distribution of those records. *These limitations are based on the qualitative difference between obtaining information from a specific case file and obtaining*

[2] "Public Access to Electronic Trial Court Records," Report to the Judicial Council of California, December 11, 2001, available at http://www.courtinfo.ca.gov/rules/reports/documents/rules06.pdf. The Rules on Public Access to Electronic Trial Court Records are available at http://www.courtinfo.ca.gov/rules/amendments/jan2002b.pdf.

> *bulk information that may be manipulated to compile personal information culled from any document, paper, or exhibit filed in a lawsuit. This type of aggregate information may be exploited for commercial or other purposes unrelated to the operations of the courts, at the expense of privacy rights of individuals*." (Emphasis added.)

Generally, the requirement that courts provide electronic access to their electronic records is conditioned on electronic access being "feasible." (E.g., Rules 2073(b),(c).)

ANALYSIS

Courts' Obligation to Protect Privacy Interests in Court Records

Courts arguably have an obligation to protect the privacy interests in the records in their stewardship. (See, e.g., *Pantos v. Superior Court* (1984) 151 Cal.App.3d 258, [court, as custodian of records, may assert privacy interests of person submitting the private information].) The primary judicial function of courts is to enforce legal obligations and redress injuries to legal rights by the determination of controversies between litigants. (*Warner v. F. Thomas Parisian Dyeing & Cleaning Works*, 105 Cal. 409, 38 P. 960.) Courts exist primarily to afford a forum for settlement of litigable matters between disputing parties. (*Vecki v. Sorensen*, 17 Cal.App.2d 390, 340, P.2d 1020.)

By participating in lawsuits, parties voluntarily submit themselves to the Court's jurisdiction in order to resolve disputes in a socially approved manner. To serve that purpose, litigants supply a great deal of sensitive personal information. In addition, many court records are obtained from members of the public who are compelled to participate in the court system involuntarily, such as defendants, jurors, and witnesses who are subpoenaed. Many times these participants must disclose their private information in court proceedings. For example, many civil and family law cases include financial information about individuals, including their account numbers or balances, tax returns, pay stubs, or Social Security numbers. Personal identifying information, such as date of birth, address, and telephone number, is included in many documents filed with the court. In addition, courts often collect sensitive personal information that has no bearing on the merits of a case, but that assists the court in contacting parties or in record keeping. Such information could include unlisted home telephone numbers, home addresses, driver's license numbers, and Social Security numbers.

Publication of such sensitive financial, medical, or family information provided by court participants could harm individuals by holding them up to ridicule, damaging their personal relationships, foreclosing business opportunities, and exposing them to identity theft.

Fair Information Principles

An overly broad policy of publishing court records risks violating two of the most basic principles of fair information practice, the principles of *purpose specification* and *use limitation*.[3] *Purpose specification* is the principle that the purposes for which personal data are collected should be specified at the time of collection and their subsequent use should be limited to those purposes or to other compatible purposes. *Use limitation* means that any use of the data other than that specified at the time of collection requires the approval of the data subject.

Participation in our judicial system should neither be interpreted, nor exploited, as a justification for wholesale sacrifice of the participant's privacy interests. Personal information in court records is obtained for a specific purpose related to the case, either because it is needed for a fair adjudication or because it is needed for administrative reasons. If courts make their records available in bulk in electronic form, they run a very strong risk that the personal information in them will be used for purposes very different from, and often incompatible with, the purposes for which the information was collected. As the public becomes aware of these incompatible uses, participants in the court process may become reluctant to freely provide personal information.

Furthermore, putting entire systems of court records on the Internet or providing them in electronic format has relatively little relevance to the public's ability to monitor the institutional operation of the courts, but has relatively great impact on the privacy of citizens who come in contact with the court as defendants, litigants, witnesses, or jurors.

We recognize the argument that a primary advantage of electronic record-keeping over paper record keeping is the increased ease of (1) extracting data from individual files that can show trends and statistics, and (2) compiling information about individuals from a large number of different files. The Office believes, however, that the public benefit of providing this type of access by bulk distribution is outweighed by the costs, particularly by the potential damage to privacy interests. As an alternative, making the records available only on a case-by-case basis would help to ensure that the aggregations that were not feasible before the records were electronic would be prevented when they are electronic.

"Practical Obscurity"

While court records may be public, providing them in bulk is qualitatively different from providing them on a case-by-case basis. Currently, those seeking information contained in court records usually must physically visit the court that has them, with the knowledge that an action

[3] Called the Fair Information Practice Principles, these widely recognized principles were first enunciated by HEW in 1973, later elaborated as Guidelines by the Organisation for Economic Cooperation and Development, and continue to represent international consensus on general guidance concerning the collection and management of personal information. By setting out core principles, the guidelines play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data.

was filed in the particular court by a specific party or against one or more specific parties. With that information, they can review the case index or register and identify documents or records, which they can then request be made available to them for their physical inspection at the court clerk's office. Getting information from court files, therefore, imposes a burden in terms of knowledge and effort. The U.S. Supreme Court has noted that information in case records enjoys what it has termed "practical obscurity."[4]

Practical obscurity provides significant privacy protection to individuals who are involved in adjudications, as demonstrated more fully in the list of issues below.

> *Risk of physical harm to victims and witnesses.* The safety of victims and witnesses could be compromised if courts were to distribute in bulk their addresses, telephone numbers, and other information that would allow them to be located. Such risk is perhaps most common in criminal and family cases.
>
> *Fraud and identity theft.* Although sensitive personal information, such as Social Security and financial account numbers, may already be available in paper files at the courthouse, its "practical obscurity" has provided it with de facto privacy protection. Distributing such information in bulk exposes it to a substantial risk of criminal misuse. Participation in court proceedings, whether voluntary or involuntary, should not expose participants to such victimization.
>
> *Determination of reliability.* Ex parte allegations, particularly in family cases, present a problem in that they may be skewed by self-interest and subsequently determined to be unreliable. Although such allegations could be read in case files at the courthouse, the physical demands of accessing such files would afford them "practical obscurity." Courts should not disseminate ex parte allegations, until there are policies and procedures to address the problems of uncontested ex parte allegations.
>
> *Statutory rehabilitation policies.* Various sections of the criminal law allow for sealing of a defendant's criminal record provided that certain conditions are met. Such sealing

[4] The United States Supreme Court in *United States Department of Justice v Reporters Committee for Freedom of the Press* (1989) 489 US 749, 109 S Ct 1468, 103 L Ed 2d 774, referred to the relative difficulty of gathering paper files as "practical obscurity." In this case, which involved a request under the Freedom of Information Act for the release of information contained in a database that summarized criminal history data, the Court recognized a privacy interest in information that is publicly available through other means, but is "practically obscure." The court noted that "the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information." It specifically commented on "the vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country, and a computerized summary located in a single clearinghouse of information." (489 US at p. 764.) In weighing the public interest in releasing personal information against the privacy interest of individuals, the court defined the public's interest as "shedding light on the conduct of any Government agency or official," rather than acquiring information about particular private citizens. (489 US at p. 773.) The court also noted "the fact that an event is not wholly private does not mean that an individual has no interest in limiting disclosure or dissemination of the information." (489 U.S. at p. 770.)

frequently does not occur by operation of law. If such information is published before conditions for sealing are met, the publication would make the subsequent sealing ineffectual and thus thwart the rehabilitative intent of the authorizing legislation. Admittedly, information could be published from files accessed at the courthouse, but the "practical obscurity" of such files has lessened the likelihood of publication and reduced the risk of thwarting rehabilitation policies. Bulk distribution of records would make it difficult to implement such policies.

Criminal cases. In September 2001, the Federal Judicial Conference[5] adopted a policy that makes criminal cases unavailable remotely for a two-year period. The Judicial Conference identified two reasons for this exclusion of criminal cases. First, electronic publication of criminal case records could jeopardize investigations that are under way and create safety risks for victims, witnesses, and their families. Second, access to pre-indictment information, such as unexecuted arrest and search warrants, could severely hamper law enforcement efforts and put law enforcement personnel at risk.

Additionally, allowing bulk distribution of criminal case information would greatly facilitate the compilation of individual criminal histories, in contravention of the public policy of some states. (See e.g., *Westbrook v. City of Los Angeles* (1994) 27 Cal.App.4th 157 [court note required to obtain access to public database containing criminal case information].) For this reason, two California Attorneys General have supported excluding criminal cases from remote electronic access:

> Our principal concern is with criminal records and the threat that the electronic release of these records poses to individual privacy and to the legislative and judicial safeguards that have been created to insure that only accurate information is disclosed to authorized recipients. (See, e.g., Penal Code sec. 11105.) The electronic dissemination of criminal records is a tremendous danger to individual privacy because it will enable the creation of virtual rap sheets or private databases of criminal proceedings, which will not be subject to the administrative, legislative or judicial safeguards that currently regulate disclosure of criminal record information. (Letter from Attorney General Daniel E. Lungren commenting on California Judicial Council's draft rules on Electronic Access to Court Records (March 6, 1997); See letter from Attorney General Bill Lockyer (Dec. 15, 2000), reaffirming position taken in March 6, 1997 letter.)

Inadvertent exposure of sensitive or personal information. Parties in the sensitive cases (e.g. family law) who are unaware that sensitive or personal information included in court filings is publicly accessible will also be unaware that they can take steps to protect such

[5] The federal court system governs itself on the national level through the Judicial Conference of the United States. The Judicial Conference … considers policy issues affecting the federal courts, makes recommendations to Congress on legislation affecting the judicial system, proposes amendments to the federal rules of practice and procedure, and considers the administrative problems of the courts. See http://www.uscourts.gov/understanding_courts/89914.htm.

information, by requesting a sealing or protective order. For example, in family law proceedings, it is not unusual for litigants to attach copies of their tax returns to their filings, even though tax returns are made confidential by statute. Similarly, in family law proceedings, allegations of abuse are not uncommon; however, litigants may not be aware that there are procedures for limiting public access to this highly sensitive and personal information to protect not only their own privacy, but also that of their minor children. The proposed bulk distribution rule threatens to sacrifice consideration of the privacy interests of litigants, particularly the self-represented, as regards sensitive or personal information that litigants have inadvertently disclosed.

Tools to apply confidentiality policies. Courts are frequently obligated by statute to protect confidential information in many types of case records. This obligation may be absolute or defined by statute or judicially determined time limits. Courts have traditionally met these obligations on an ad hoc basis, as individual case records have been requested at the courthouse. To produce records in bulk in a responsible manner, courts would need to meet these obligations by applying appropriately protective criteria to all records, not only those that are requested on a case-by-case basis. Many courts simply do not have staff who can review and appropriately expurgate all records to make them available for bulk distribution, and reliable, automated methods to review and expurgate records do not presently exist. Until such automated methods can be developed and applied by case management systems, the proposed rules should not make bulk distribution available.

Advantages of a "Case-by-Case" Approach

The case-by-case approach adopted by the California Judicial Council and endorsed by the Office of Privacy Protection recognizes that court resources are limited and that providing either a searchable database or bulk distribution of court records would entail costs. Courts should not invest their limited resources to provide such data, which may be used for private purposes that have nothing to do with the function of the court, the reasons for making court records open to public access, or the reasons for which the information was obtained. The courts have a strong public policy reason for making case data available upon request to persons seeking information about a particular case. Court case management systems are designed to retrieve and display case data based on a request noting the name of a party or the case number. Many, if not most, case management systems are currently not designed to provide bulk case data or to compile information except on a very limited basis. In theory, any case management system can be programmed to return any data desired. In practice, the determination of what data is obtainable is often sharply limited by the cost of modifying the case management system to provide the data.

The case-by-case approach also avoids some of the practical limitations with data interpretation that are posed by definitional and historical problems. Commentary included in the Model Policy Draft on Access to Compiled Information from Court Records (Section 4.50) notes that compiled data presents two significant problems in interpretation. First, "Analysis of the data without an

understanding of the meaning of the data elements or codes used, or without an understanding [of] the limitations of the data can result in conclusions not substantiated by the data." Second, electronic records can represent a skewed set of data that results from norms that have not been applied consistently to all case types or over the entire span of time covered by the case inventory.

In other words, computer-generated reports will be unreliable if data elements have not been clearly defined and the definitions consistently applied. Case management systems frequently do not apply standard data definitions consistently across all case types. Even if they did, a correct interpretation of the reports would require explanatory materials that normally do not exist in standardized form. For the foreseeable future, case-by-case access would obviate these problems.

Finally, any bulk distribution scheme would be vulnerable to human error. Recent inadvertent bulk disclosures of highly sensitive and private information demonstrate that any database is vulnerable to compromise through human error. For example, on June 27, 2001, Eli Lilly sent an email to people enrolled in a Prozac electronic reminder program typically used to alert them to refill their prescriptions. Each message inadvertently included the addresses for all the other patients on the list. The online identities of some 600 people were thus compromised. Given patients' sensitivity about disclosures of medical information, such as the fact that they're taking a drug prescribed for mental illness, the privacy breach was particularly damaging. It is important to note that this data distribution error could have been avoided if the employee who handled the details of distributing the email had listed the recipients in the data entry block designed for "bcc" recipients, rather than in the "cc" block.

To guard against such errors, and to maintain public confidence in the courts' institutions, courts will be constrained to undertake data vulnerability assessments, implement appropriate administrative controls, and educate employees about the need and ways to shield personal data. Courts may find it prudent to develop sound encryption programs and effective data firewalls, develop contingency plans for data security breaches, and make some court official personally responsible for data security.

Regarding Proposed Rule 8.10 – Dissemination of Information to Litigants About Access to Information in Court Records

The Office of Privacy Protection believes that Model Rule 8.10 should be amended to alert litigants to the availability of limitations on the access to and distribution of personal information that they have submitted in connection with their causes.

As discussed above, parties to lawsuits (particularly family law contests) are frequently unaware that sensitive or personal information included in court filings may be publicly accessible. Such parties are also frequently unaware that procedures may be available to them by which they might protect such information, by requesting a sealing or protective order.

Proposed Rule 8.10 goes only part of the way needed to address these problems. In addition to warning litigants that court records may be publicly accessible, we believe that Rule 8.10 should provide for a notice to alert litigants to the existence of procedures that will enable them to seek to have sensitive, confidential or personal information on them redacted before the records are made accessible to the public. The addition of such a notice would promote the integrity of courts as responsible custodians of such information.

The fair information practice principles at issue here are *openness* and *use limitation*. *Openness* is the general policy that should prevail in the handling of personal information. Practices such as the subject's opportunity to seek limits on disclosure of his or her personal information should be made explicit. As explained above, the principle of use limitation requires the consent of, and hence notice to, the data subject before the data can be disclosed for purposes other than those specified at the time of collection. Including a notice as recommended here is critical to litigants' ability to ask for limits on the uses of their sensitive personal information; without such a notice, the practical effect of model Rule 8.10 is seriously undercut.

Respectfully submitted,

Joanne B. McNabb, Chief
California Office of Privacy Protection

April 30, 2002